

UNITED STATES DISTRICT COURT

for the

District of Northern Mariana Islands

FILED
Clerk
District Court

JUL 20 2010

For The Northern Mariana Islands
By [Signature]
(Deputy Clerk)
MAY 05 2021

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Email account [Redacted]

Case No.

MC 10-00049

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the _____ District of the Northern Mariana Islands (identify the person or describe property to be searched and give its location):

See paragraph 3, Affidavit in Support of Search Warrant of SA Michael Janiga.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Affidavit in Support of Search Warrant of SA Michael Janiga, attachment "A"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 371, 666, 1343, and the application is based on these facts:

Conspiracy,
 Theft or Bribery concerning programs receiving federal funds, and Fraud

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[Signature]
 Applicant's signature

Michael J. Janiga Special Agent
 Printed name and title

Sworn to before me and signed in my presence.

Date:

19 July 2010

City and state:

Saipan, CNMI

[Signature]
 Judge's signature

Honorable Robert J. Bryan
 Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Michael Janiga, being first duly sworn on oath, state the following:

A. Introduction and Agent Background

1. I am currently a Special Agent for the United States Environmental Protection Agency (hereinafter "EPA"), Office of Inspector General (hereinafter "OIG"), Western Resource Center, San Francisco, California. I have been employed as a law enforcement agent with the EPA OIG for approximately two years. Prior to that, I was employed with various other federal agencies for 21 years as a Special Agent in both management and non-management positions, conducting and coordinating fraud investigations involving federal programs.

2. As a Special Agent for the EPA OIG, my responsibilities include conducting investigations of alleged criminal violations of environmental statutes, as well as federal violations of Title 18 of the United States Code, including Conspiracy (Title 18, United States Code, Section 371), Theft or Bribery concerning programs receiving federal funds (Title 18, United States Code, Section 666), and Fraud by wire, radio, or television (Title 18, United States Code, 1343.

3. Based on the facts contained in this Affidavit, my participation in this investigation, including witness interviews conducted by myself, with and/or other law enforcement agents, information obtained from the Federal Bureau of Investigation as a result of its investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience, I believe there is probable cause to conclude that records evidencing the violations of Title 18, United States Code, Sections 371 (Conspiracy), 666 (Theft or Bribery concerning programs receiving federal funds), and 1343 (Wire Fraud) are located on an account controlled by the web-based electronic communications provider known as Yahoo! Inc, (hereinafter "Yahoo", located at 701 First Avenue, Sunnyvale, California 94089. The account to be searched is [REDACTED], which is further described in "Attachment A". I believe that the email addresses [REDACTED], is associated with an individual named **Franz Benjamin Reksid**, who is a Special Assistant to the Secretary of the Department of Public Lands (hereinafter "DPL") located on the Island of Saipan in the Commonwealth of the Northern Mariana Islands (hereinafter "CNMI"). As set forth herein, there is probable cause to believe that on the computer systems of Yahoo, there exists evidence, fruits, and instrumentalities of violations of Title

18, United States Code, Sections 371 (Conspiracy), 666 (Theft or Bribery concerning programs receiving federal funds), and 1343 (Wire Fraud).

4. In my training and experience, I have learned that Yahoo is a company that provides web based Internet electronic mail ("email") access to the general public, and that stored electronic communications, including opened and unopened email for Yahoo subscribers, may be located on the computers of Yahoo. Further, I am aware that computers maintained by Yahoo contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seek authorization to search the email and other information stored on the Yahoo servers for the computer account and files and following the search procedure described in Attachment A, Section I and II, and to seize the information described in Attachment A, Section III.

B. Search Procedure

5. In order to facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and the accompanying application for search warrant seeks authorization to permit employees of Yahoo to assist agents in the execution of this warrant. Pursuant to 18 U.S.C. § 2703(g) my presence, or the presence of an Agent, is not

required for service or execution of a warrant issued under 18 U.S.C. § 2703. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Yahoo personnel who will be directed to isolate those accounts and files described in Section II of Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, Yahoo employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact duplicate of all information stored in the computer accounts and files described in Section II of Attachment A;

c. Yahoo employees will provide the exact duplicate in electronic form of the accounts and files described in Section II of the Attachment A and all information stored in those accounts and files to the Agent who serves this search warrant; and

d. Accordingly, this affidavit and application for search warrant seek authorization to search the email and other information stored on the Yahoo servers for the computer account and files and following the search procedure described in Attachment A, Section I and II, and to seize the information described in Attachment A, Section III.

C. Background Regarding Computers, the Internet, and Email

6. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

7. I have experience investigating computer-related crimes. Based on my experience, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web ("www") is a functionality of the Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is typically initiated at the user's computer, transmitted to the subscriber's mail server, and then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

D. Yahoo

8. Based on my training and experience, I have learned the following about Yahoo:

a. Yahoo provides an email service which is available free of charge to Internet users. Subscribers obtain an account by registering via the Internet with Yahoo;

b. Yahoo maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information;

c. Yahoo requests subscribers to provide basic information, which may include name, gender, zip code and other personal/biographical information. However, to the best of my

knowledge Yahoo does not verify the registration information provided;

d. Subscribers to Yahoo can access their accounts on servers maintained and/or owned by Yahoo from computers connected to the Internet around the world;

e. A Yahoo subscriber seeking to send email can use a web-based interface to log into the account, type the message, and then submit it to Yahoo's mail servers for transmission to its recipient(s). Similarly, a Yahoo subscriber seeking to read a received message can use a web-based interface to log into the account and view the message on Yahoo's servers;

f. A Yahoo subscriber may elect to download and store on his or her personal computer copies of email messages or other files sent or received via the account. In addition to, or instead of, downloading such data to a local computer, a Yahoo subscriber may elect to remotely store copies of email messages or other files sent or received via the account on Yahoo's servers for subsequent retrieval. Accordingly, a search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the Yahoo server, and vice versa;

g. Any email that is sent to a Yahoo subscriber is stored in the subscriber "mail box" on Yahoo servers until the subscriber deletes the email or the subscriber mail box exceeds

the storage limits set by Yahoo. If the message is not deleted and the account size is below the maximum limit, that message can remain on the Yahoo servers indefinitely. Similarly, Yahoo subscribers have the option of saving a copy of sent email; unless the subscriber specifically deletes the email from the Yahoo server, it can remain on the system indefinitely as long as the account size is under the maximum limit. In addition, Yahoo permits subscribers to sign up for linked services such as My Photos and Flickr. These services allow subscribers to store pictures and other files remotely on Yahoo servers, where they remain indefinitely as long as the account size is under the maximum limit. I know from my training and experience that users sometimes save attached photos and files to linked accounts.

h. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Yahoo may not be. I also know that the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Yahoo employees may not be. It would be inappropriate and impractical, however, for federal agents to search the vast computer network of Yahoo for the relevant accounts and then to analyze the contents of those accounts on

the premises of Yahoo. The impact on Yahoo's business would be severe;

i. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Yahoo, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Yahoo to make a digital copy of the entire contents of the information subject to search specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A; and

j. Executing a warrant to search a Yahoo account requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject email account in this case for evidence of the target crimes will require that agents cursorily inspect all emails produced by Yahoo in order to ascertain which contain evidence of those crimes, just as it necessary for Agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents in order to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to ensure that law enforcement can discover all information subject

to seizure pursuant to Section III of Attachment A. Keywords search text, but many common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

E. Stored Wire and Electronic Communication Access

9. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental

entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection-

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under

investigation or equivalent State
warrant

(2) Paragraph (1) is applicable with
respect to any electronic communication that
is held or maintained on that service-

(A) on behalf of, and received by
means of electronic transmission
from (or created by means of
computer processing of
communications received by means
of electronic transmission from),
a subscriber or customer of such
remote computing service; and

(B) solely for the purpose of
providing storage or computer
processing services to such
subscriber or customer, if the
provider is not authorized to
access the contents of any such
communications for purposes of
providing any services other than
storage or computer processing.

3) Pursuant to 18 U.S.C. § 2703(c)(2), the government

may also use a warrant to obtain the following information from a provider of electronic communication service or remote computing service:

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

4) In addition to the information specified above, the government may also obtain records and other information pertaining to a subscriber or customer of electronic

communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A).

e. No notice to the subscriber or customer is required when the government obtains information under either 18 U.S.C. § 2703(c)(1) or (2). 18 U.S.C. § 2703(c)(3).

f. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter -

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

g. Title 18, United States Code, Section 2510, provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

14) "electronic communications

system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; .

. . .

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;.

(17) "electronic storage" means --

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such

communication by an electronic
communication service for
purposes of backup protection
of such communication.

h. Title 18, United States Code, Section 2703(g) provides as follows: "[n]otwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber or to customer of such service."

F. Source of Information Contained Herein

10. I have been assisted in this investigation by the Federal Bureau of Investigation (hereinafter "FBI") who is currently conducting an investigation into Franz B. Reksid's activities.

G. Probable Cause

11. On October 09, 2009 Special Agent James Barry, FBI, Saipan Resident Agency, CNMI informed me that he was conducting an investigation involving **Franz Benjamin Reksid**, date of birth

[REDACTED] 1940, physical address Chalan Kanoa District, #3, Saipan, MP 96950, for Wire Fraud.

12. Special Agent Barry informed me that he met with Investigators Ed Pua and Erwin Flores of the CNMI Attorney General's Investigative Unit (hereinafter "AGIU") on November 10, 2009 who informed him they served a search warrant on the Fast Cash Pawn Shop, San Jose, Saipan, a Western Union non-bank financial institution on October 26, 2009 and obtained records revealing that Reksid and an associate (who is also one of Reksid's victims) had transmitted \$339,818.00 from Saipan to the Ivory Coast of Africa and possibly other foreign countries between January 21, 2009 and October 12, 2009.

13. Special Agent Barry informed me that Investigators Pua and Erwin told him that Reksid had borrowed \$146,089.96 from eight friends and associates by escorting them to ATMs for cash and to bank loan officers in order for them to take out loans for him. Special Agent Barry informed me he learned that Reksid obtained the funds by telling his victims he needed the money to pay for funeral arrangements for family members in Palau, medical procedures for his wife, or for his wife's gambling debts. Special Agent Barry informed me that the whereabouts \$193,728.04 of Reksid's Western Union wire transfers remained unexplained.

14. Prior to my initial contact with Special Agent Barry,

Assistant Special Agent in Charge (hereinafter "ASAC") Dean Tsukada, U.S. Department of Interior OIG, informed me that he and Special Agent Barry had conducted interviews at the CNMI Department of Public Lands (hereinafter "DPL"), which is Reksid's place of employment. ASAC Tsukada informed me that DPL was funding projects in the CNMI using EPA Brownfields grant funds. ASAC Tsukada informed me that Reksid had oversight of the Brownfields program funds and the United States Attorney's Office on Saipan was seeking assistance with an investigation to determine if Reksid had converted federal funds to his personal use, potentially accounting for some or all of the \$193,728.04 of unexplained wire transfers.

15. I know that the CNMI receives funds from the Federal government through EPA to develop and execute projects under the Brownfields program. The Brownfields program, which is implemented by EPA, was created in 2001 by the U.S. Congress pursuant to Public Law 107-118 (The Small Business Liability Relief and Brownfields Revitalization Act. In effect, the legislation amends the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 to "promote the cleanup and reuse of brownfields, to provide financial assistance for brownfields revitalization, to enhance State response programs and for other purposes...". More specifically, "[b]rownfields are real property, the expansion, redevelopment, or reuse of

which may be complicated by the presence or potential presence of a hazardous substance, pollutant, or contaminant. Cleaning up and reinvesting in these properties protects the environment, reduces blight, and takes development pressures off greenspaces and working lands."

16. On December 09, 2009, I contacted Anna Woods, Financial Specialist, EPA Las Vegas Finance Center (hereinafter "LVFC") to discuss Brownfields grants reimbursements made by EPA to DPL. I know from my EPA employment that the LVFC provides grants financial management and accounting services to grant recipients in support of the U.S. Environmental Protection Agency's mission with responsibilities. LVFC Grants financial management responsibilities include payment processing, financial closeout, and the development of policies, procedures, and systems to assist EPA grant recipients during the life of the grant.

17. Woods told me that in 2006 EPA awarded DPL Brownfields grant #BF-96984701, totaling \$550,000.00, to conduct environmental site assessments (hereinafter "ESAs") of lands on Saipan potentially contaminated with petroleum and unexploded ordinance (hereinafter "UXO"). Woods further informed me that in 2008, EPA awarded DPL Brownfields grant #BF-96988401, totaling \$200,000 to clean-up the UXO discovered during the UXO ESAs. Woods explained to me that EPA grants management

regulations permitted DPL to draw money down from the EPA through the LVFC via electronic funds transfer to a DPL dedicated bank account, after DPL reimbursed its contractors for work performed on the Brownfields grants. Woods also explained to me that EPA grants management regulations permitted DPL to request an advance of funds from EPA through the LVFC through and electronic funds transfer to a dedicated DPL bank account, to pay its contractors. In the latter example EPA grants management regulations required DPL to pay its contractors costs within 72 hours of the receipt of the advanced funds.

18. Woods informed me that \$200,000 of Brownfields grant BF-96984701 was awarded by DPL to three contractors to perform Petroleum ESAs and the remaining \$350,000 of Brownfields grant #BF-96984701 was used by DPL to award a contract to AMPRO, LLC, Saipan, MP (hereinafter "AMPRO") to conduct UXO ESAs. Woods told me that DPL awarded an additional \$200,000 to AMPRO in 2008 through EPA Brownfields grant #BF96988401 to perform UXO clean-up.

19. I learned from reviewing the above mentioned EPA grant files, stored in the EPA Regional Office in San Francisco, California, and from receiving and reviewing documents provided to me by Reksid and other DPL employees, and John Scott, President, AMPRO, that AMPRO was awarded DPL contract #EA07-017 on October 01, 2007 from funding to be reimbursed by Brownfields

grant #BF96984701. The contract was valued at \$297,152.00. DPL later modified contract #EA07-017 based on a change order on March 01, 2009 from funding to be reimbursed by Brownfields grant #BF-96988401, awarding an additional \$200,000.00 to AMPRO, for a total of \$497,152.00.

20. On December 08, 2009 I interviewed John Scott in the presence of Special Agent Barry and Scott's Father-in-Law at a bar and grill establishment on Saipan. John Scott informed me that Reksid had approached him on multiple occasions asking him for "loans" after DPL had reimbursed AMPRO on its invoices for work performed in accordance with the contract specifications. John Scott told me he denied Reksid's requests for loans on each occasion. John Scott told me that he was aware that Reksid had recently been arrested for borrowing money from people living on Saipan.

21. In late January or early February 2010, I spoke with Pankaj Arora who is the EPA Brownfield's Program Officer responsible for overseeing the progress of EPA Brownfield's grants #BF-96984701 and #BF-96988401. I am aware that Pankaj Arora travels to the CNMI and regularly meets with DPL employees Reksid, Mario Cepeda, a subordinate employee to Reksid in the Brownfields program and Margaret Villagomez, the Manager of Accounting Services, to review the progress of the work performed using the Brownfields grants and to assure DPL

employees are managing the grant funds in compliance with Title 40 of the Code of Federal Regulations entitled, "Protection of Environment".

22. Pankaj Arora told me that Mario Cepeda had recently contacted him by telephone to complain that Reksid was using Cepeda's DPL computer for unknown reasons. Pankaj Arora told me that Mario Cepeda informed him that he suspected Reksid was misusing the computer for personal reasons because he was aware that Reksid was recently charged and arrested by the CNMI Attorney General's Office, and that subsequently Reksid's DPL authorities and computer access was taken away. Pankaj Arora told me that Cepeda had initially given Reksid his computer password in fear of retaliation by Reksid, to include being fired from his job and eventually informed Reksid he could no longer use his computer, however: Cepeda told Arora that Reksid continued to gain access to the computer.

23. On February 12, 2010, Special Agent Barry informed me that he interviewed Mario Cepeda after I informed him of my conversation with Pankaj Arora. Special Agent Barry informed me that Mario Cepeda said Reksid began using Cepeda's computer prior to Reksid's arrest. I learned that Reksid was sent a message from one Fadil Hamdi on August 11, 2009, which message was received through Cepeda's DPL email account. According to

Cepeda, although Reksid erased his computer transactions on Cepeda's DPL computer, Cepeda obtained one of Reksid's messages with the assistance of a DPL computer specialist. Cepeda provided Special Agent Barry with a copy of the email, which was forwarded to me. It reads, in part: "[b]ear in mind that we are dealing with the government, any lapses from your side could cost us this project." Reksid replied:

"I will do my best to send it tomorrow. I was not able to find anything today. I will let you know by tomorrow before noon. Try NOT to send email to my regular email address. My computer and email is being monitored by the federal people for wire fraud. So send email to me using this email address of my assistant ([REDACTED]). Sorry for the inconvenience. Thank you. Regards, Franz".

24. The content of this email indicates to me that Reksid was secretly communicating from Mario Cepeda's DPL computer to discuss projects funded by DPL where Reksid had oversight, including projects potentially funded by the EPA. Reksid's communication also indicates to me that he wanted to hide information concerning business transactions from federal law enforcement officials because he was aware that he was being investigated.

25. On April 28, 2010, I interviewed Reksid in the presence of Special Agent Barry at the FBI Resident Agency Office on Saipan to discuss potential contract improprieties involving him and John Scott and to learn if he had borrowed

money from Scott for his personal use while managing DPL contract #EA07-017. Reksid told me that he shared with John Scott a Work Plan developed by DPL encompassing the contract specification for completing the UXO ESAs and other tasks Scott was to perform for DPL as its prime contractor. Reksid told me that Work Plan included a breakdown of the costs for each of the tasks John Scott was to perform and Scott used the Work Plan to create his scope of work for the completion of the ESAs. Reksid further informed me that he included language in DPL contract #EA07-017 that benefited John Scott and AMPRO to increase his profit margin, by reimbursing Scott for Business Gross Revenue Taxes, ultimately adding five percent to the \$497,152.00 Scott would earn from DPL contract #EA07-017.

26. Reksid informed me in his interview that he reviewed Scott's performance on only six occasions and paid AMPRO invoices without determining first if John Scott had completed the work he billed DPL for. I am aware from invoices that I have received from John Scott and later reviewed, that AMPRO has submitted claims for reimbursement to DPL on at least 15 occasions. Reksid also told me that he borrowed \$3000.00 from John Scott for his personal use and had not repaid Scott to date.

27. Special Agent Barry asked Reksid about his current

financial debts attributed to borrowing money from people he knows on Saipan. Reksid told Special Agent Barry that he had a great deal of debt from paying for several family member funerals. Reksid admitted to Special Agent Barry that he had sent money overseas but would not provide the total sum he was in debt.

28. On April 28, 2010, approximately two hours after completing Reksid's interview, Pankaj Arora contacted me from his EPA Office in San Francisco, California to inform me that he was speaking with Mario Cepeda via telephone when Reksid returned from his interview at the FBI office. Pankaj Arora told me Mario Cepeda said that Reksid began using Cepeda's computer soon after returning to the DPL office from the FBI office and that Reksid used his personal email account [REDACTED] to send email messages from Cepeda's computer. Pankaj Arora said that Mario Cepeda was not aware of whom Reksid was sending email messages to. Pankaj Arora informed me that Cepeda told him that a DPL computer specialist working in the DPL Information Technology office had previously applied software to Cepeda's computer on the DPL computer network in order to capture Reksid's incoming and outgoing messages, while he was using Cepeda's. Pankaj Arora provided me with Mario Cepeda's cellular telephone number, (670) [REDACTED] so

I could verify with Cepeda what he had just informed Arora of.

29. On April 28, 2010, Special Agent Barry, in my presence, contacted Mario Cepeda at cellular telephone number (670) [REDACTED] to discuss his telephone conversation that day with Pankaj Arora about Reksid accessing Cepeda's computer using personal email account.

30. After his conversation with Mario Cepeda, Special Agent Barry told me that Cepeda confirmed with him what he had previously told Pankaj Arora and informed Barry that Reksid's personal email address was [REDACTED]. Special Agent Barry informed me that Mario Cepeda did not know to whom Reksid was sending email messages.

31. On April 28, 2010, approximately five hours after completing Reksid's interview at the FBI Office on Saipan, John Scott contacted me at my EPA email address from his AMPRO business email address and stated, "I hear you're on island asking questions about the Marpi Brownfield project. I'm currently on Guam and will be on Saipan most of next week. I'm available if you have questions regarding the project." John Scott's email message indicated to me that Reksid was in contact with Scott possibly using Mario Cepeda's computer and Reksid's personal email account after his interview. Neither Special Agent Barry nor I had contacted Scott to make him aware of

Reksid's interview at the FBI Office on Saipan that day.

32. Reksid contacted me by telephone on April 29, 2009 and confirmed he received the \$3000.00 loan from John Scott in February 2009, nine months prior to my December, 08, 2009 interview with Scott. Reksid told me that during his telephone conversation with John Scott that Scott acknowledged giving him the money and that Scott was not concerned with a timely repayment of the debt by Reksid.

33. On May 05, 2010 I interviewed John Scott telephonically from my EPA office in San Francisco, California while Scott sat with Special Agent Barry in the FBI Office on Saipan. John Scott told me he provided Reksid \$3000.00 on February 12, 2009, depositing the money into Reksid's First Hawaiian Bank account at the Maite bank branch on Guam. John Scott reiterated from his December 08, 2009 interview that Reksid had asked him for money on several other occasions, usually after Scott was paid for contract services by DPL. John Scott told me he was not truthful during his December 08, 2009 interview about giving Reksid money because he wanted to avoid the appearance that he was giving Reksid a kickback.

34. I learned on May 06, 2010 from William Downer, Assistant Attorney General, Office of the Attorney General, CNMI, who provided CNMI Superior Court Records to me that Reksid

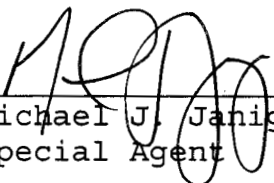
was charged with a criminal information and arrested on September 29, 2009 under criminal case number 09-182D for two felony counts of theft by deception for borrowing money from two of his victims with no intention of repaying them. The charges were subsequently dismissed for unknown reasons.

H. Conclusion

35. Based upon the information above, I submit that there is probable cause to believe that on the computer systems owned, maintained, and/or operated by Yahoo, headquartered at, 701 First Avenue, Sunnyvale, California 94089, there exists evidence, fruits, and instrumentalities of violations of Title 18 United States Code, Sections 371, 1343, and 666. I believe a search warrant of Reksid's Yahoo email account will reveal emails to co-conspirators, to include John Scott, incriminating statements, and evidence of obstruction of a federal investigation concerning Wire Fraud and Theft or Bribery concerning programs receiving federal funds. By this affidavit and application, I request that the Court issue a search warrant directed to Yahoo allowing agents to search the email and other information stored on the Yahoo servers for the computer accounts and files and following the search procedure described in Attachment A, Section I and II, and to seize the information described in Attachment A, Section III.

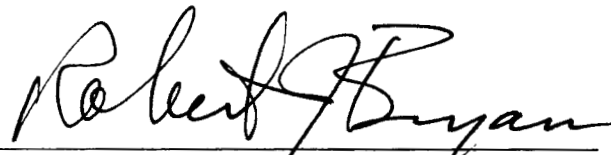
I. Request for Sealing

36. Since this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.



Michael J. Janiga
Special Agent

Sworn to and subscribed before me
on this 19 day of July, 2010



United States ~~Magistrate~~ Judge
District

ATTACHMENT A

I. Search Procedure

- A. The search warrant will be presented to Yahoo, Inc (“Yahoo”) personnel who will be directed to isolate those accounts and files described in Section II below;
- B. In order to minimize any disruption of computer service to innocent third parties, Yahoo employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II below, including an exact duplicate of all information stored in the computer accounts and files described therein;
- C. Yahoo employees will provide the exact duplicate in electronic form of the accounts and files described in Section II below and all information stored in those accounts and files to the agent who serves the search warrant; and
- D. Law Enforcement personnel will thereafter review all information and records received from Yahoo employees to determine the information to be seized by law enforcement personnel specified in section III below.

II. Files and Accounts to be Copied by Yahoo Employees

- A. The contents of any and all wire and electronic communications, including attachments and stored files, for the account [REDACTED] (“subscriber”) including received messages, sent messages, deleted messages, stored draft messages, messages maintained in trash or other folders, Yahoo Talk messages, and existing printouts from original storage of all of the wire and electronics communications for the subscriber account;
- B. Any and all contents of electronic files that the subscriber has stored in the subscriber’s Documents and Picasa areas;
- C. Any and all Yahoo IDs listed on the subscriber’s Contact list;
- D. Account information for the subscriber’s account including:
 - 1. Names and associated e-mail addresses;
 - 2. Physical address and location information;
 - 3. Records of session times and durations;
 - 4. Length of service (including start date) and types of service utilized;
 - 5. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;
 - 6. The means and source of payment for such service including any credit card or bank account number); and

7. Internet Protocol address used by the subscriber to register the account or otherwise initiate service.
- E. User connection logs for the subscriber account, for any connection to or from the subscriber account. User connection logs should include the following:
1. Connection time and date;
 2. Disconnect time and date;
 3. Method of connection to system (e.g. SLIP, PPP, Shell);
 4. Data transfer volume (e.g., bytes);
 5. The IP address that was used when the user connect to the service;
 6. Connection information for other systems to which the user connected via the subscriber account, including:
 - a. Connection destination
 - b. Connection time and date;
 - c. Disconnect time and date;
 - d. Method of connection to system (e.g. telnet, ftp, http);
 - e. Data transfer volume (e.g., bytes);
 - f. Any other relevant routing information;
 - g. Source or destination of any wire or electronic mail messages sent from or received by the subscriber account, and the date , time, and length of the message; and
 - h. Any address to which the wire or electronic communication was or is to be forwarded from the subscriber account or e-mail address. If any such messages are forwarded to an IP address associated with a TCP/IP connection from another account or IP address assigned to Yahoo or any corporate affiliate thereof, please provide the records described in Section II.D and II.E for that account as well.

III. Information to be Seized by Law Enforcement Personnel

- A. The contents of any and all wire and electronic communications, including attachment and stored files, header information, described in Section II.A. (above), which relate in any manner, directly or indirectly, to electronic correspondence involving illegal wire transfer of funds and the misuse of federal grant funds in violation of Title, 18 United States Code, Section 371, 666, and 1343.
- B. All of the records and information describe above in Sections II.B –II.E.